(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 11041231 A

(43) Date of publication of application: 12.02.99

(51) Int. Cl H04L 9/32
G09C 1/00
G09C 1/00
H04L 9/08

(21) Application number: 09208447

(22) Date of filing: 17.07.97

(71) Applicant: NIPPON TELEGR & TELEPH CORP <NTT>

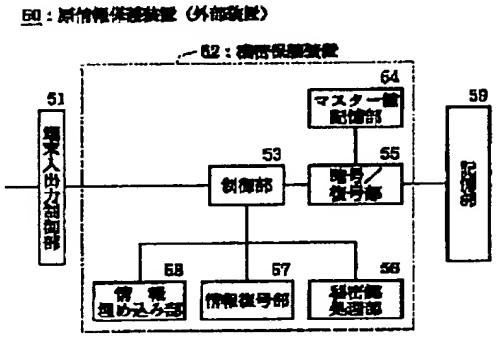
(72) Inventor: TAKADA SHUNSUKE
NAKAMURA TAKAO
OGAWA HIROSHI
KAWAKUBO HIDEJI

(54) ORIGINAL INFORMATION PROTECTION METHOD AND DEVICE FOR INFORMATION DISTRIBUTION SYSTEM

(57) Abstract:

PROBLEM TO BE SOLVED: To prevent a user from copying illicitly the original information based on the purchased encipherment information by using an external device to decode the enciphered distributed information, to embed a user authenticator into the decoded original information and also to manage the keys which are used for both decoding and embedding processes.

SOLUTION: This original information protection device (external device) 50 consists mainly of an information decoding part 57 and an information embedding part 58. When the device 50 is produced, a master key that is inherent to the device 50 is stored in a master key storage part 54 of a security device 52. At an enciphering/decoding part 55, a user's secret key is enciphered by the master key that is stored in the part 54 and this enciphered key is stored in a storage part 59. The control part of a user terminal receives the enciphered key via an open key and sends this received key to the device 50. A terminal input/output control part 51 of the device 50 sends the received key to a control part 53.



Express Mail EL039790667US

(19)日本国特許庁(JP)　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平１１－４１２３１

(43)公開日　平成11年(1999)2月12日

(51)Int.Cl.[6]		識別記号	FI		
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６７５　Ａ
Ｇ０９Ｃ	1/00	６４０	Ｇ０９Ｃ	1/00	６４０　Ｄ
		６６０			６６０　Ａ
Ｈ０４Ｌ	9/08		Ｈ０４Ｌ	9/00	６０１　Ａ
					６０１　Ｅ

審査請求　未請求　請求項の数７　ＦＤ　（全９頁）　最終頁に続く

(21)出願番号　特願平９－２０８４４７

(22)出願日　平成9年(1997)7月17日

(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番2号

(72)発明者　高田　俊介
東京都新宿区西新宿三丁目19番2号　日本電信電話株式会社内

(72)発明者　中村　高雄
東京都新宿区西新宿三丁目19番2号　日本電信電話株式会社内

(72)発明者　小川　宏
東京都新宿区西新宿三丁目19番2号　日本電信電話株式会社内

(74)代理人　弁理士　川久保　新一

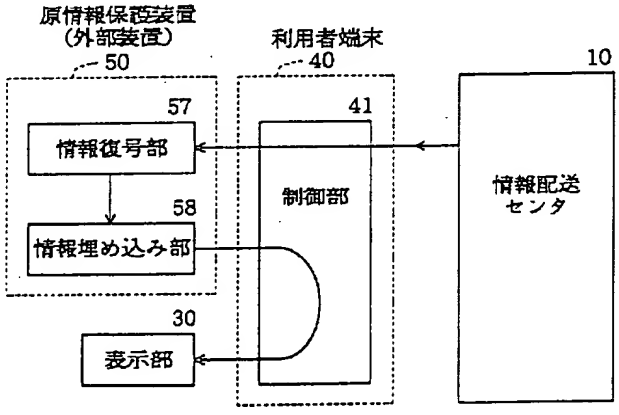
最終頁に続く

(54)【発明の名称】情報流通システムにおける原情報保護方法およびその装置

(57)【要約】

【課題】　情報流通システムにおいて、利用者が購入した暗号化情報に基づいて、利用者が原情報を不正複製することを阻止することができる原情報保護方法およびその装置を提供することを目的とするものである。

【解決手段】　暗号化されている流通情報を復号する処理を利用者端末の外部装置で実行させ、また、復号した原情報に利用者認証子を埋め込む処理を上記外部装置で実行させ、さらに、上記復号処理と上記埋め込む処理とに使用する鍵を上記外部装置が管理するものである。



1

【特許請求の範囲】

【請求項１】　情報流通システムにおいて、

暗号化されている原情報を復号する原情報復号手段と；上記復号された原情報に、情報埋め込み鍵によって利用者認証子を埋め込む利用者認証子埋め込み手段と；を有し、上記原情報復号手段と、上記利用者認証子埋め込み手段とが、利用者端末の外部に設けられていることを特徴とする情報流通システムにおける原情報保護装置。

【請求項２】　請求項１において、

上記原情報復号の処理と上記利用者認証子埋め込みの処理とに使用する鍵を管理することを特徴とする情報流通システムにおける原情報保護装置。

【請求項３】　請求項１において、

公開鍵暗号方式の利用者公開鍵によって情報配送センタで暗号化した情報暗号鍵、情報埋め込み鍵、利用者認証子を、利用者秘密鍵によって復号する復号手段と；上記復号された情報暗号鍵、情報埋め込み鍵、利用者認証子を記憶する記憶手段と；を有することを特徴とする情報流通システムにおける原情報保護装置。

【請求項４】　請求項１において、

秘密鍵処理部と情報復号部と情報埋め込み部とを具備する機密保護装置を有し、

上記秘密鍵処理部は、情報配送センタにおいて利用者の公開鍵で暗号化された情報暗号鍵、情報埋め込み鍵、利用者認証子を復号するものであり、

上記情報復号部は、上記情報配送センタで暗号化された情報を、上記情報暗号鍵によって復号するものであり、

上記情報埋め込み部は、上記利用者認証子を復号した情報に埋め込む装置であることを特徴とする情報流通システムにおける原情報保護装置。

【請求項５】　情報流通システムにおいて、

マスター鍵記憶部と暗号／復号部とを具備する機密保護装置と、記憶部とを有し、

上記暗号／復号部は、上記記憶部に情報を送信するときに、上記マスター鍵記憶部に格納してあるマスター鍵で暗号化し、上記記憶部から情報を受信するときに復号する装置であることを特徴とする情報流通システムにおける原情報保護装置。

【請求項６】　情報流通システムにおいて、

暗号化されている原情報を復号する原情報復号段階と；上記復号された原情報に、情報埋め込み鍵によって利用者認証子を埋め込む利用者認証子埋め込み段階と；を有し、上記原情報復号段階と、上記利用者認証子埋め込み段階とが、利用者端末の外部で実行されることを特徴とする情報流通システムにおける原情報保護方法。

【請求項７】　情報流通システムにおいて、

暗号化されている原情報を復号する原情報復号手段と；上記復号された原情報に、情報埋め込み鍵によって利用者認証子を埋め込む利用者認証子埋め込み手段と；としてコンピュータを機能させるためのプログラムを記録したコンピュータ読取可能な記録媒体。

2

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、情報流通システムにおいて、原情報を保護する方法およびその装置に関する。

【０００２】

【従来の技術】従来の情報流通システムＩＦＳにおいて、利用者が情報配送センタから流通情報を購入する場合、利用者が上記流通情報を不正に二次利用することを抑止するために、利用者が流通情報を購入し、この流通情報を復号した原情報に利用者認証子を埋め込む方式が採用されている。なお、上記不正の例としては、プログラムの改竄や、利用者端末または情報配送センタへの不正が考えられる。

【０００３】図４は、従来の情報流通システムＩＦＳを示すブロック図である。

【０００４】図５は、上記従来例の動作を示す図である。

【０００５】情報流通システムＩＦＳにおいて、情報配送センタ１０で原情報が暗号化され、情報配送センタ１０から利用者が暗号化された原情報を購入し、利用者端末２０において、原情報が復号され、この復号された原情報が表示部３０に表示される。なお、利用者端末２０は、制御装置２１を有し、この制御装置２１は、暗号化された原情報を復号する復号部２２と、復号された原情報に利用者認証子を埋め込む情報埋め込み部２３とを有する。

【０００６】上記のように、復号した原情報に利用者認証子を埋め込むようにすれば、その原情報を二次利用すると、その原情報に利用者認証子がついて回るので、利用者はその情報を二次利用することができない。

【０００７】

【発明が解決しようとする課題】しかし、上記従来例において、利用者端末で利用者が不正することによって、利用者認証子が埋め込まれていない原情報を入手することが可能である。

【０００８】つまり、従来の情報流通システムにおいて、暗号化された原情報を情報配送センタから利用者が購入した後、暗号化された原情報を復号鍵によって復号し、この復号された原情報に利用者認証子が埋め込まれるのに先立って、上記復号鍵や復号された原情報がメモリ上に一時的に展開される。ここで、この復号鍵や復号された原情報を抽出するプログラムや装置を、利用者が自分の利用者端末にしかけることが可能である。すなわち、暗号化された情報を復号化するプログラムや、復号化された原情報をハードディクス等に落すプログラムを利用者が作り、このようなプログラムを使用することによって、復号された原情報を利用者が入手することができる。

【０００９】また、復号用の鍵が利用者に盗まれた場合、利用者認証子が原情報に埋め込まれる前に、暗号化情報が原情報に復号され、この原情報が利用者に入手されるという問題がある。

【００１０】この結果、復号された原情報が利用者によって不正に複製され、その利用者が、複製した原情報を再び流通させること等が可能になり、原情報の提供者の利益が損なわれるという問題がある。

【００１１】本発明は、情報流通システムにおいて、利用者が購入した暗号化情報に基づいて、利用者が原情報を不正複製することを阻止することができる原情報保護方法およびその装置を提供することを目的とするものである。

【００１２】

【課題を解決するための手段】本発明は、暗号化されている流通情報を復号する処理を利用者端末の外部装置で実行させ、また、復号した原情報に利用者認証子を埋め込む処理を上記外部装置で実行させ、さらに、上記復号処理と上記埋め込む処理とに使用する鍵を上記外部装置が管理するものである。

【００１３】

【発明の実施の形態および実施例】図１は、本発明の一実施例である原情報保護装置（外部装置）５０を、利用者端末４０と情報配送センタ１０とともに示すブロック図である。

【００１４】原情報保護装置（外部装置）５０は、主に、情報復号部５７と、情報埋め込み部５８とを有するものであり、ＩＣカード、ＰＣカード等の計算機用カード、またはボード等の形態を有するものである。

【００１５】初期条件としては、次のようなものである。まず、情報配送センタ１０は、公開鍵暗号方式の秘密鍵Ｋｃｓを持ち、公開鍵Ｋｃｐを公開している。利用者は、公開鍵暗号方式の秘密鍵Ｋｕｓを持ち、公開鍵Ｋｕｐを公開している。

【００１６】外部装置５０を製造するときに、機密保護装置５２内のマスター鍵記憶部５４に、装置固有のマスター鍵Ｋｍを格納する。

【００１７】マスター鍵記憶部５４に記憶されているマスター鍵Ｋｍによって、暗号／復号部５５において、利用者の秘密鍵Ｋｕｓが暗号化され、このマスター鍵Ｋｍで暗号化された秘密鍵Ｋｍ［Ｋｕｓ］が記憶部５９に格納される。

【００１８】また、情報配送センタ１０は、流通情報Ｍを登録し、情報Ｍに対する暗号鍵Ｋｅと情報埋め込み鍵Ｋｗとを生成し、暗号鍵Ｋｅによって情報Ｍにスクランブルを施し、暗号化情報Ｋｅ［Ｍ］を生成する。また、情報配送センタ１０は、スクランブルが施された流通情報Ｋｅ［Ｍ］を流通させる。

【００１９】一方、利用者端末４０における制御部４１は、スクランブルが施された流通情報Ｋｅ［Ｍ］を受信し、この受信した流通情報Ｋｅ［Ｍ］を表示部３０に表示し、スクランブルが施された流通情報Ｋｅ［Ｍ］を閲覧する。そして、流通情報Ｋｅ［Ｍ］を利用者が購入する場合、購入要求と、利用者認証子Ｕｉｄと、パスワードＰｗとを、情報配送センタ１０に送信する。

【００２０】なお、上記処理の代わりに、次のように処理するようにしてもよい。つまり、まず、情報提供者は、情報Ｍと、情報Ｍを容易に想像することができるサイズが小さい情報Ｍ’（画像情報の場合はサイズを小さくした画像情報、プログラムやゲーム等の場合は体験版等）とを作成し、これら情報Ｍと、サイズが小さい情報Ｍ’とを情報配送センタ１０に登録し、情報配送センタ１０は、サイズが小さい情報Ｍ’を流通させる。そして、利用者から購入要求があると、情報配送センタ１０は、暗号鍵Ｋｅと情報埋め込み鍵Ｋｗとをランダムに生成し、情報Ｍを暗号鍵Ｋｅで暗号化し、この暗号鍵Ｋｅで暗号化された情報Ｋｅ［Ｍ］を生成する。その後、暗号鍵Ｋｅ、情報埋め込み鍵Ｋｗ、利用者認証子Ｕｉｄを利用者の公開鍵で暗号化したものと、暗号化情報Ｋｅ［Ｍ］とを、利用者に送信するようにしてもよい。

【００２１】情報配送センタ１０は、利用者認証子ＵｉｄとパスワードＰｗとに基づいて利用者認証を行う。また、流通情報Ｍの暗号鍵Ｋｅと情報埋め込み鍵Ｋｗと利用者認証子Ｕｉｄとを、それぞれ、利用者の公開鍵Ｋｕｐによって暗号化し、公開鍵Ｋｕｐによって暗号化された暗号鍵Ｋｕｐ［Ｋｅ］、公開鍵Ｋｕｐによって暗号化された情報埋め込み鍵Ｋｕｐ［Ｋｗ］、公開鍵Ｋｕｐによって暗号化された利用者認証子Ｋｕｐ［Ｕｉｄ］を生成する。そして、これら生成された公開鍵Ｋｕｐによって暗号化された暗号鍵Ｋｕｐ［Ｋｅ］、公開鍵Ｋｕｐによって暗号化された情報埋め込み鍵Ｋｕｐ［Ｋｗ］、公開鍵Ｋｕｐによって暗号化された利用者認証子Ｋｕｐ［Ｕｉｄ］を利用者端末４０に送信する。

【００２２】図２は、原情報保護装置５０の具体例を示すブロック図である。

【００２３】原情報保護装置（外部装置）５０は、端末入出力制御部５１と、機密保護装置５２と、記憶部５９とを有する。機密保護装置５２は、制御部５３と、マスター鍵記憶部５４と、暗号／復号部５５と、秘密鍵処理部５６と、情報復号部５７と、情報埋め込み部５８とを有する。

【００２４】次に、上記実施例における利用者側の動作について説明する。

【００２５】図３は、上記実施例の動作を示すフローチャートである。

【００２６】まず、利用者端末４０の制御部４１は、公開鍵Ｋｕｐによって暗号化された暗号鍵Ｋｕｐ［Ｋｅ］を受信し、この暗号鍵Ｋｕｐ［Ｋｅ］を外部装置５０に送信し、外部装置５０の端末入出力制御部５１は、上記暗号鍵Ｋｕｐ［Ｋｅ］を、制御部５３に渡す。そして、

マスター鍵Ｋｍで暗号化された秘密鍵Ｋｍ［Ｋｕｓ］が記憶部５９に格納されており、この格納されている秘密鍵Ｋｍ［Ｋｕｓ］を、マスター鍵記憶部５４に格納されているマスター鍵Ｋｍによって暗号／復号部５５が復号するように、制御部５３が制御し、秘密鍵Ｋｕｓが得られる。

【００２７】また、公開鍵Ｋｕｐによって暗号化された暗号鍵Ｋｕｐ［Ｋｅ］を、利用者の秘密鍵Ｋｕｓによって、秘密鍵処理部５６が復号するように、制御部５３が制御し、暗号鍵Ｋｅが得られる。マスター鍵Ｋｍによって、暗号／復号部５５が暗号鍵Ｋｅを暗号化し、この暗号化された暗号鍵Ｋｍ［Ｋｅ］を記憶部５９に格納するように、制御部５３が制御する。また、暗号鍵Ｋｍ［Ｋｅ］の格納場所を識別する識別子Ｋｅ－ＩＤを、制御部５３が、端末入出力制御部５１から制御部４１へ返す。

【００２８】そして、公開鍵Ｋｕｐによって暗号化された情報埋め込み鍵Ｋｕｐ［Ｋｗ］、公開鍵Ｋｕｐによって暗号化された利用者認証子Ｋｕｐ［Ｕｉｄ］についても、上記処理と同様の処理を行い、マスター鍵Ｋｍによって暗号化された情報埋め込み鍵Ｋｍ［Ｋｗ］、マスター鍵Ｋｍによって暗号化された利用者認証子Ｋｍ［Ｕｉｄ］を、記憶部５９に格納し、情報埋め込み鍵Ｋｍ［Ｋｗ］、利用者認証子Ｋｍ［Ｕｉｄ］の格納場所を識別する識別子Ｋｗ－ＩＤ、Ｕｉｄ－ＩＤを、制御部５３が、端末入出力制御部５１から制御部４１へ返す。

【００２９】次に、利用者端末４０の制御部４１は、受信した暗号化情報Ｋｅ［Ｍ］と識別子Ｋｅ－ＩＤとを外部装置５０へ送信し、端末入出力制御部５１は、暗号化情報Ｋｅ［Ｍ］を制御部５３に渡す。

【００３０】制御部５３は、記憶部５９に格納されている暗号鍵Ｋｍ［Ｋｅ］を、識別子Ｋｅ－ＩＤに基づいて抽出し、暗号／復号部５５が、この抽出された暗号鍵Ｋｍ［Ｋｅ］をマスター鍵Ｋｍで復号し、暗号鍵Ｋｅを得る。暗号鍵Ｋｅによって暗号化情報Ｋｅ［Ｍ］を情報復号部５７が復号し、情報Ｍを得るように制御部５３が制御する。また、マスター鍵Ｋｍによって情報Ｍを暗号／復号部５５が暗号化し、記憶部５９に格納し、暗号化情報Ｋｍ［Ｍ］を得るように、制御部５３が制御する。

【００３１】そして、制御部５３は、暗号化情報Ｋｍ［Ｍ］の格納場所を識別する識別子Ｍ－ＩＤを、端末入出力制御部５１から制御部４１へ返す。制御部４１は、識別子Ｍ－ＩＤ、Ｋｗ－ＩＤ、Ｕｉｄ－ＩＤを外部装置５０へ送信し、端末入出力制御部５１は、上記情報を制御部５３に渡す。記憶部５９に格納された暗号化鍵Ｋｍ［Ｋｗ］、暗号化利用者認証子Ｋｍ［Ｕｉｄ］、記憶部５９に格納された暗号化情報Ｋｍ［Ｍ］を、識別子Ｋｗ－ＩＤ、Ｕｉｄ－ＩＤ、Ｍ－ＩＤによって抽出し、暗号／復号部５５がマスター鍵Ｋｍで復号し、鍵Ｋｗ、利用者認証子Ｕｉｄ、情報Ｍを得るように、制御部５３が制御する。

【００３２】また、情報埋め込み部５８が、鍵Ｋｗによって情報Ｍに利用者認証子Ｕｉｄを埋め込み、利用者認証子Ｕｉｄが埋め込まれた情報Ｋｗ［Ｍ］を生成するように、制御部５３が制御する。端末入出力制御部５１から、利用者認証子Ｕｉｄが埋め込まれた情報Ｋｗ［Ｍ］を制御部４１に返すように、制御部５３が制御し、外部装置５０から返却された利用者認証子Ｕｉｄ埋め込み情報Ｋｗ［Ｍ］を表示部３０が表示するように、制御部４１が制御する。

【００３３】なお、端末入出力制御部５１から利用者認証子Ｕｉｄ埋め込み情報Ｋｗ［Ｍ］を制御部４１に返し、外部装置５０から返却された利用者認証子Ｕｉｄ埋め込み情報Ｋｗ［Ｍ］を表示部３０が表示する代わりに、次のように処理してもよい。つまり、暗号／復号部５５が、利用者認証子Ｕｉｄが埋め込まれた情報Ｋｗ［Ｍ］をマスター鍵Ｋｍによって暗号化し、暗号化情報Ｋｍ［Ｋｗ［Ｍ］］を生成し、記憶部５９に格納し、格納場所を識別する識別子Ｋｗ［Ｍ］－ＩＤを、制御部４１に返すように、制御部５３が制御し、制御部４１から、識別子Ｋｗ［Ｍ］－ＩＤと表示命令とを受信したときに、識別子Ｋｗ［Ｍ］－ＩＤによって、記憶部５９から暗号化情報Ｋｍ［Ｋｗ［Ｍ］］を抽出し、暗号化情報Ｋｍ［Ｋｗ［Ｍ］］を暗号／復号部５５がマスター鍵Ｋｍで復号し、利用者認証子Ｕｉｄが埋め込まれた情報Ｋｗ［Ｍ］を生成し、端末入出力制御部５１から制御部４１へ返すように処理するようにしてもよい。

【００３４】また、上記実施例において、情報流通システムにおいて、暗号化されている原情報を復号する原情報復号手段と、復号された原情報に、情報埋め込み鍵によって利用者認証子を埋め込む利用者認証子埋め込み手段とを有し、上記原情報復号手段と上記利用者認証子埋め込み手段とが、利用者端末の外部に設けられていれば、情報流通において利用者が購入した情報から原情報を抽出することを防止することができる。

【００３５】この場合、原情報復号の処理と利用者認証子埋め込みの処理とに使用する鍵を原情報保護装置が管理するようにすれば、利用者による原情報抽出を確実に防止することができる。

【００３６】また、公開鍵暗号方式の利用者公開鍵によって情報配送センタで暗号化した情報暗号鍵、情報埋め込み鍵、利用者認証子を、利用者秘密鍵によって復号する復号手段と、上記復号された情報暗号鍵、情報埋め込み鍵、利用者認証子を記憶する記憶手段とを原情報保護装置に持たせれば、利用者による原情報抽出をより確実に防止することができる。

【００３７】さらに、秘密鍵処理部と情報復号部と情報埋め込み部とを具備する機密保護装置を有し、上記秘密鍵処理部は、情報配送センタにおいて利用者の公開鍵で暗号化された情報暗号鍵、情報埋め込み鍵、利用者認証子を復号するものであり、上記情報復号部は、上記情報

配送センタで暗号化された情報を、上記情報暗号鍵によって復号するものであり、上記情報埋め込み部は、上記利用者認証子を復号した情報に埋め込む装置であるようにすれば、利用者による原情報抽出をさらに確実に防止することができる。

【００３８】また、マスター鍵記憶部と暗号／復号部とを具備する機密保護装置と、記憶部とを有し、上記暗号／復号部は、上記記憶部に情報を送信するときに、上記マスター鍵記憶部に格納してあるマスター鍵で暗号化し、上記記憶部から情報を受信するときに復号する装置であるようにすれば、利用者による原情報抽出をより一層確実に防止することができる。

【００３９】なお、上記実施例を方法の発明として把握することができる。つまり、上記実施例は、情報流通システムにおいて、暗号化されている原情報を復号する原情報復号段階と、上記復号された原情報に、情報埋め込み鍵によって利用者認証子を埋め込む利用者認証子埋め込み段階とを有し、上記原情報復号段階と、上記利用者認証子埋め込み段階とが、利用者端末の外部で実行される情報流通システムにおける原情報保護方法である。

【００４０】また、上記実施例を記録媒体の発明として把握することができる。つまり、上記実施例は、情報流通システムにおいて、暗号化されている原情報を復号する原情報復号手段と、上記復号された原情報に、情報埋め込み鍵によって利用者認証子を埋め込む利用者認証子埋め込み手段ととしてコンピュータを機能させるためのプログラムを記録したコンピュータ読取可能な記録媒体である。

【００４１】

【発明の効果】本発明によれば、情報流通システムにおいて、利用者が購入した暗号化情報に基づいて、利用者が原情報を不正複製することを阻止することができるという効果を奏する。

【図面の簡単な説明】

【図１】本発明の一実施例である原情報保護装置（外部装置）５０を、利用者端末１０と情報配送センタ１０とともに示すブロック図である。

【図２】原情報保護装置５０の具体例を示すブロック図である。

【図３】上記実施例の動作を示すフローチャートである。

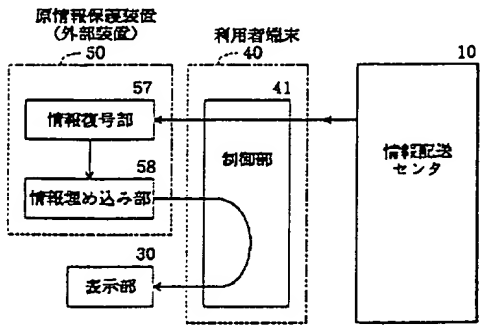
【図４】従来の情報流通システムＩＦＳを示すブロック図である。

【図５】上記従来例の動作を示す図である。

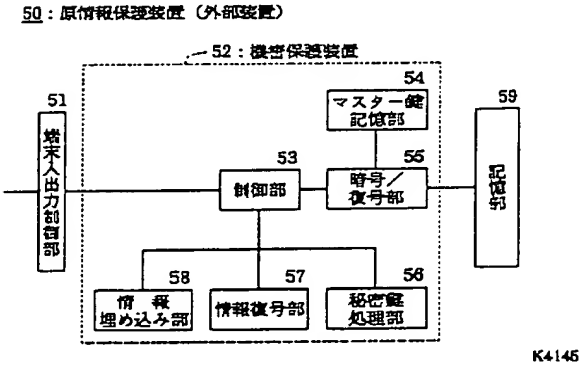
【符号の説明】

１０…情報配送センタ、
３０…表示部、
４０…利用者端末、
４１…制御部、
５０…原情報保護装置、
５１…端末入出力制御部、
５２…機密保護装置、
５３…制御部、
５４…マスター鍵記憶部、
５５…暗号／復号部、
５６…秘密鍵処理部、
５７…情報復号部、
５８…情報埋め込み部、
５９…記憶部。

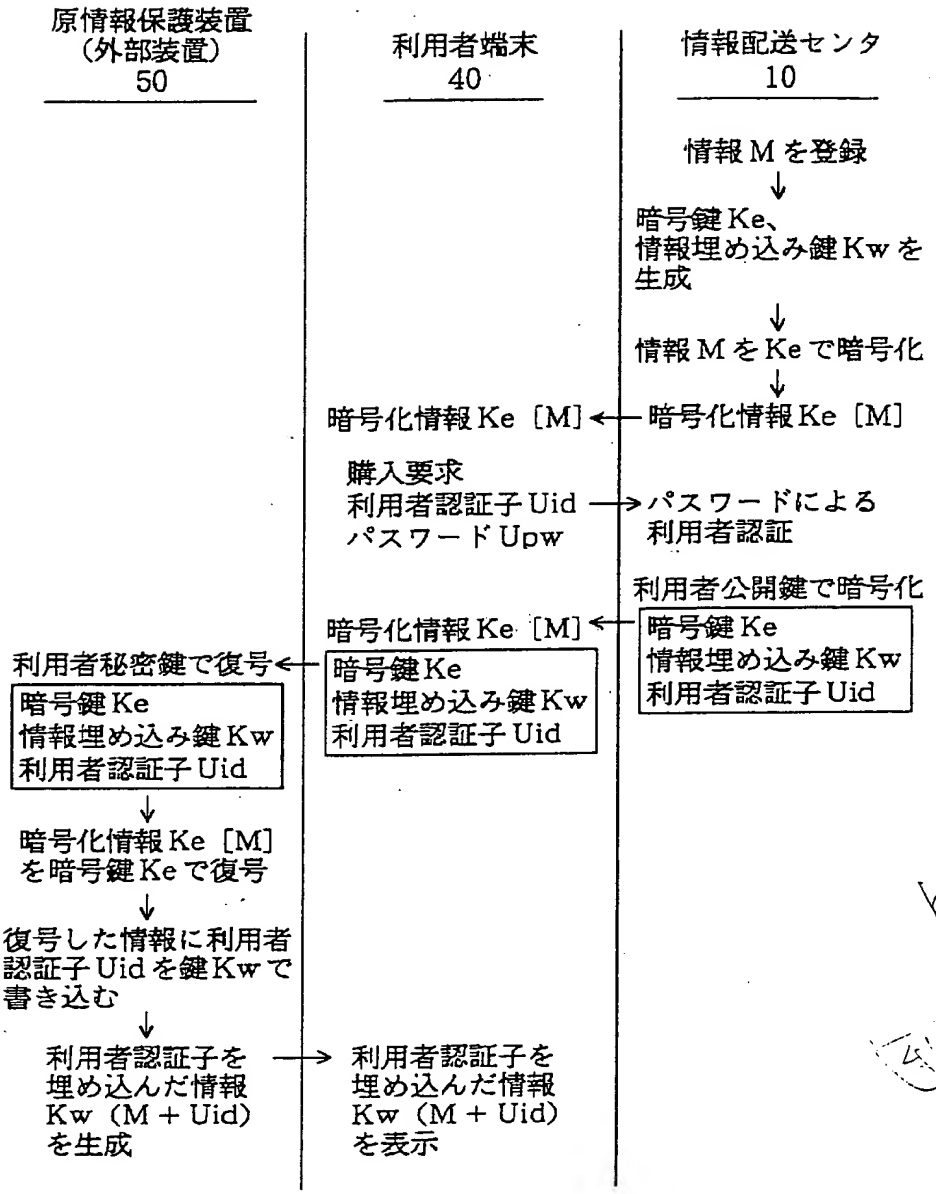
【図１】



【図２】



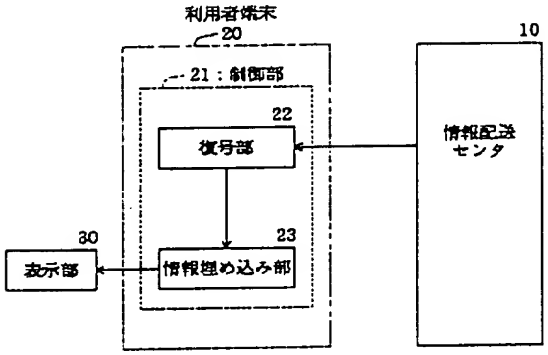
【図３】


原情報保護装置
(外部装置)
50
利用者端末
40
情報配送センタ
10
情報Mを登録
暗号鍵Ke、
情報埋め込み鍵Kwを
生成
情報MをKeで暗号化
暗号化情報Ke［M］
暗号化情報Ke［M］
購入要求
利用者認証子Uid
パスワードUpw
パスワードによる
利用者認証
利用者公開鍵で暗号化
暗号化情報Ke［M］
暗号鍵Ke
情報埋め込み鍵Kw
利用者認証子Uid
利用者秘密鍵で復号
暗号鍵Ke
情報埋め込み鍵Kw
利用者認証子Uid
暗号化情報Ke［M］
を暗号鍵Keで復号
復号した情報に利用者
認証子Uidを鍵Kwで
書き込む
利用者認証子を
埋め込んだ情報
Kw（M＋Uid）
を生成
利用者認証子を
埋め込んだ情報
Kw（M＋Uid）
を表示

K4145

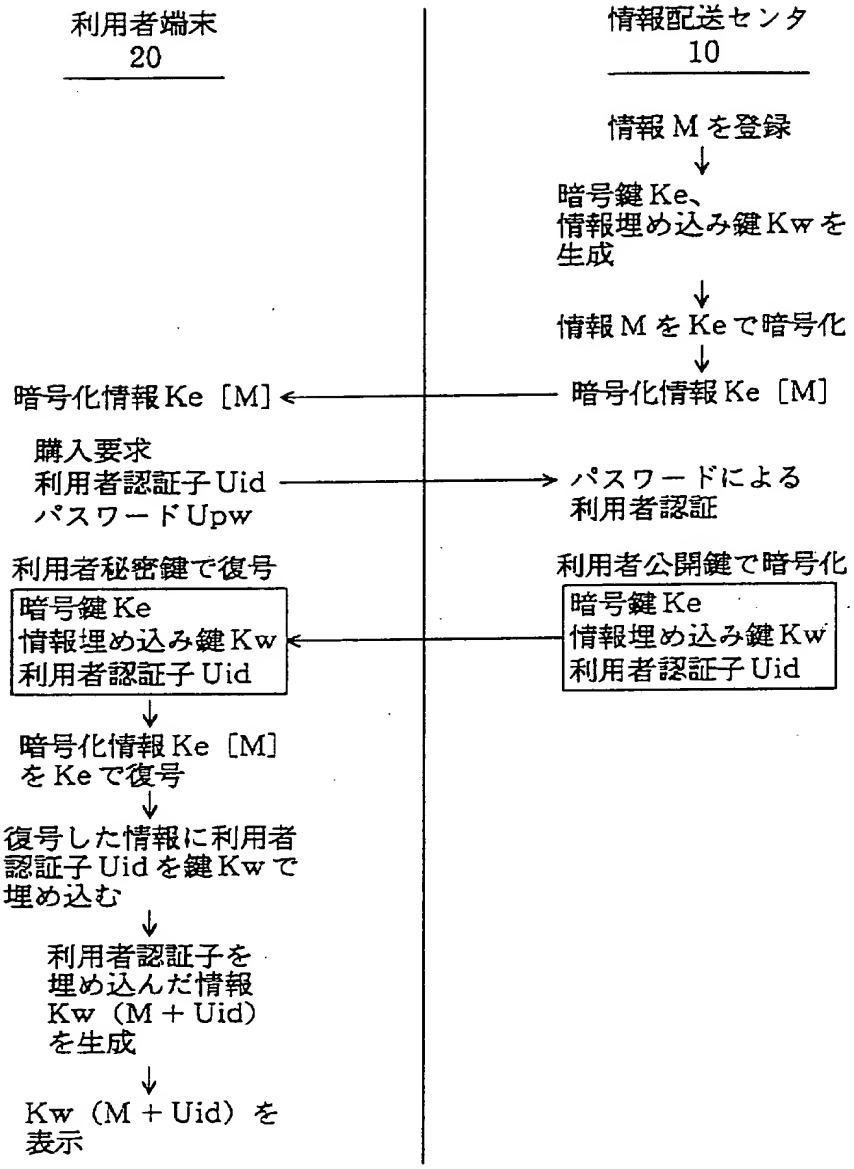
【図４】

IFS：従来の情報流通システム



K4145

【図５】



K4145

フロントページの続き

(51)Int.Cl.⁶	識別記号	FI	
		H04L 9/00	675D

(72)発明者　河久保　秀二
東京都新宿区西新宿三丁目19番２号　日本
電信電話株式会社内